

Polynomial-time isomorphism test of groups that are tame extensions

Joshua A. Grochow*

Youming Qiao†

July 10, 2015

Abstract

We give new polynomial-time algorithms for testing isomorphism of a class of groups given by multiplication tables (GPI). Two results (Cannon & Holt, J. Symb. Comput. 2003; Babai, Codenotti & Qiao, ICALP 2012) imply that GPI reduces to the following: given groups G, H with characteristic subgroups of the same type and isomorphic to \mathbb{Z}_p^d , and given the coset of isomorphisms $\text{Iso}(G/\mathbb{Z}_p^d, H/\mathbb{Z}_p^d)$, compute $\text{Iso}(G, H)$ in time $\text{poly}(|G|)$. Babai & Qiao (STACS 2012) solved this problem when a Sylow p -subgroup of G/\mathbb{Z}_p^d is trivial. In this paper, we solve the preceding problem in the so-called “tame” case, i.e., when a Sylow p -subgroup of G/\mathbb{Z}_p^d is cyclic, dihedral, semi-dihedral, or generalized quaternion. These cases correspond exactly to the group algebra $\mathbb{F}_p[G/\mathbb{Z}_p^d]$ being of tame type, as in the celebrated tame-wild dichotomy in representation theory. We then solve new cases of GPI in polynomial time.

Our result relies crucially on the divide-and-conquer strategy proposed earlier by the authors (CCC 2014), which splits GPI into two problems, one on group actions (representations), and one on group cohomology. Based on this strategy, we combine permutation group and representation algorithms with new mathematical results, including bounds on the number of indecomposable representations of groups in the tame case, and on the size of their cohomology groups.

Finally, we note that when a group extension is *not* tame, the preceding bounds do not hold. This suggests a precise sense in which the tame-wild dichotomy from representation theory may also be a dividing line between the (currently) easy and hard instances of GPI.

1 Introduction

The group isomorphism problem GPI is to decide whether two finite groups, given by their multiplication tables, are isomorphic. It is one of the few natural problems not known to be in P, and unlikely to be NP-complete, as it reduces to Graph Isomorphism (GRAPHI; see, e.g., [33]). In addition to its intrinsic interest, resolving the exact complexity of GPI is thus a tantalizing question. Further, there is a surprising connection between GPI and the Geometric Complexity Theory program (see, e.g., [38] and references therein): Techniques from GPI were used to solve cases of LIE ALGEBRA ISOMORPHISM that have applications in Geometric Complexity Theory [23]. In a survey article [2] in 1995, after enumerating several isomorphism-type problems including GRAPHI

*Santa Fe Institute, Santa Fe, NM, USA, jgrochow@santafe.edu

†Centre for Quantum Computation and Intelligent Systems, University of Technology, Sydney, Australia, jimmyqiao86@gmail.com

and GPI, Babai expressed the belief that GPI might be the only one expected to be in P.¹ Despite its connection with GRAPHI, P seems an achievable goal for GPI, as there are many reasons GPI seems easier than GRAPHI (see, e. g., the introduction to [24] for an overview of these reasons).

As a group of order n can be generated by $\lceil \log n \rceil$ elements, GPI is solvable in time $n^{\log n + O(1)}$ [19, 37].² The only improvement for the general case was Rosenbaum’s recent $n^{0.5 \log n + O(1)}$ [42]. However, there have been more significant improvements for special group classes, representing a more structural approach to the problem. Isomorphism of Abelian groups was recognized as easy quite early [43, 46], leading to an $O(n)$ -time algorithm [32]. Since 2009, there have been several non-trivial polynomial-time algorithms for much more complicated group classes: groups with no Abelian normal subgroups [3, 4], groups with Abelian Sylow towers [34, 40, 5], and quotients of generalized Heisenberg groups [35].

Partly motivated to distill a common pattern from the three recent major polynomial-time algorithms [4, 5, 35], the authors proposed [24] a divide-and-conquer strategy for GPI based on the extension theory of groups. This strategy is crucial for Theorem 1. Before getting to the details of this strategy, let us first examine an approach for GPI that motivates the problem that we study.

In 2003, Cannon and Holt [13] suggested the following outline for GPI. First, they introduce a natural sequence of characteristic subgroups: $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_\ell = \text{id}$, where $G_1 = \text{Rad}(G)$ is the solvable radical of G —the largest solvable normal subgroup—and G_i/G_{i+1} is elementary Abelian for all $1 \leq i \leq \ell - 1$. This filtration is easily computed, and for each factor we know how to test isomorphism: $G/\text{Rad}(G)$ has no Abelian normal subgroups, so is handled by [4].

Given two groups G and H , after computing these filtrations of G and H , the strategy is to first test isomorphisms of the corresponding factors, which is necessary for G and H to be isomorphic. Then, starting from $G_0/G_1 (= G/\text{Rad}(G))$, proceed inductively along this filtration. Note that for G_0/G_1 , not only is isomorphism decidable in polynomial time, but a generating set for the coset of isomorphisms $\text{Iso}(G_0/G_1, H_0/H_1)$ can be found in polynomial time [4]. After this initial step, a positive solution to the following problem would show that $\text{GPI} \in \text{P}$:

Problem 1. Given two groups G, H with characteristic elementary Abelian subgroups A and B , respectively, compute $\text{Iso}(G, H)$ from $\text{Iso}(G/A, H/B)$ in time $\text{poly}(|G|)$.

In fact, by developing a heuristic algorithm for Problem 1 in [13, Sec. 5], Cannon & Holt obtained a practical algorithm for GPI, but their algorithm uses a backtrack search that does not have good worst-case guarantees.³ Still, this is a very natural approach, and the polynomial-time algorithm for testing isomorphisms for $G/\text{Rad}(G)$ [4] solves the first step to this approach in the Cayley table model.

To the best of our knowledge, the only previous result about Problem 1 with a worst-case analysis in the Cayley table model is by Babai and the second author [5], who solved the case when $A \cong \mathbb{Z}_p^k$ and the Sylow p -subgroup⁴ of G/A is trivial; that is, when $p \nmid |G/A|$. This was the key to the main result in [5].

¹The exact quotation from Babai’s 1995 survey [2] is: “None of the problems mentioned in this section, with the possible exception of isomorphism of groups given by a Cayley table, is expected to have polynomial time solution.”

²Miller [37] attributes this algorithm to Tarjan.

³Due to different goals and settings, it is natural that our setting and the setting of Cannon & Holt use different algorithmic ideas. That is, Cannon & Holt work with more succinct representations of groups, and their goal is to obtain algorithms fast in practice, even if only heuristically. We work with the more “redundant” Cayley tables, but our goal is worst-case analysis.

⁴Although Sylow p -subgroups of a group need not be unique, for a given p they are all isomorphic, so we may speak of “the” Sylow p -subgroup unambiguously, when we only need to refer to its isomorphism type.

In this paper, we solve Problem 1 under certain conditions on the Sylow subgroups of G , more general than the aforementioned one for [5]. Furthermore, these conditions are very natural, as they are aligned with the celebrated tame-wild dichotomy in the representation theory of associative algebras [17, 8].

The following is a high-level picture of the tame-wild dichotomy; defining tame and wild rigorously requires terminology that is unnecessary for this article; we refer to [8, Sec. 4.4] for a comprehensive introduction. For an algebra L over an infinite field, classifying its indecomposable representations up to isomorphism—those representations that are not direct sums of smaller ones—is a fundamental problem. The nicest possibility is when there are only finitely many indecomposables, in which case L is said to be of *finite type*. Beyond this, some algebras have the property that their indecomposables come in finitely many one-parameter families in each fixed dimension d ,⁵ possibly with finitely many exceptions. While this can be much more complicated than finite type, it is still “classifiable;” such algebras are said to be of *tame type*.⁶ Finally, some algebras L have the surprising property that any indecomposable representation of *any* algebra can be “embedded as” (or “simulated by”) an indecomposable of L ; such algebras are called *wild*. Drozd’s celebrated dichotomy theorem [18] says that every algebra over an algebraically closed field is either tame or wild.

In the case of groups, there is an explicit description of the three cases (see [8, Theorem 4.4.4]): let p be the characteristic of the field \mathbb{F} . $\mathbb{F}G$ is of finite type if and only if $p = 0$, or $p > 0$ and the Sylow p -subgroup of G is cyclic. G is of tame type, but not finite, if and only if $p = 2$ and the Sylow 2-subgroup of G is dihedral, semi-dihedral, or generalized quaternion (see Section 2 for definitions). All other cases are wild.

Suppose a group G has a normal subgroup A isomorphic to \mathbb{Z}_p^d , and let $Q = G/A$. G is called a *tame extension* of A by Q , if $\overline{\mathbb{F}}_p Q$ is of tame type.⁷ We solve Problem 1 exactly for groups of this form. Note that the Sylow p -subgroup being cyclic already generalizes the condition for [5].

Theorem 1. *Suppose G, H come from the class of groups that have characteristic subgroups of the same type and isomorphic to the elementary Abelian subgroup \mathbb{Z}_p^d . There is a polynomial-time algorithm to compute the coset of isomorphisms $\text{Iso}(G, H)$ from the coset of isomorphisms $\text{Iso}(G/\mathbb{Z}_p^d, H/\mathbb{Z}_p^d)$, if G is a tame extension of \mathbb{Z}_p^d , namely if the Sylow p -subgroups of G/\mathbb{Z}_p^d are cyclic, dihedral, semi-dihedral, or generalized quaternion.*

The condition on G/\mathbb{Z}_p^d is satisfied by several well-known group classes:

- Groups with dihedral Sylow 2-subgroups are classified [22, 7]: Let $O(G)$ be the maximal normal odd-order subgroup. If G has a dihedral Sylow subgroup, $G/O(G)$ must be isomorphic to one of: (i) a subgroup of $\text{PTL}_2(\mathbb{F}_q)$ containing $\text{PSL}_2(\mathbb{F}_q)$;⁸ (ii) the alternating group A_7 ; (iii) a Sylow 2-subgroup of G .

⁵For readers not familiar with this concept, here is an example to illustrate intuitively what one-parameter families mean. For an algebraically closed field \mathbb{F} , the Jordan blocks form a one-parameter family with the eigenvalue $\lambda \in \mathbb{F}$ as the parameter. The indecomposable d -dimensional representations of $\mathbb{F}[x]$ are given exactly by the $d \times d$ Jordan blocks.

⁶Note that finite type can be considered as a special case of tame type, namely when the number of one-parameter families is 0. In the literature, some authors take the definition of “tame type” to explicitly exclude finite type. We do not adopt that approach here.

⁷ $\overline{\mathbb{F}}_p$ is the algebraic closure of \mathbb{F}_p . Although it is not standard to apply “tame” to extensions, this slight abuse is justified by the mathematical results behind our main theorem.

⁸ $\text{PTL}_n(\mathbb{F}_q)$ is the semi-direct product $\text{PGL}_n(\mathbb{F}_q) \rtimes \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, where the Galois group $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acts on $n \times n$ matrices by sending each entry α to α^p , where p is the unique prime dividing q .

- The Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$ is generalized quaternion when q is odd [21, p. 42] (or see [15, Corollary 4.12]).
- If D is a division ring, then any Sylow subgroup of a finite subgroup of the unit group $D \setminus \{0\}$ is cyclic or generalized quaternion (see [15, Corollary 4.10]).
- The Sylow 2-subgroups of the following groups are semi-dihedral: $\mathrm{PSL}_3(\mathbb{F}_q)$ for $q \equiv 3 \pmod{4}$, $\mathrm{PSU}_3(\mathbb{F}_q)$ for $q \equiv 1 \pmod{4}$, the Mathieu group M_{11} , and $\mathrm{GL}_2(\mathbb{F}_q)$ for $q \equiv 3 \pmod{4}$ (see, e. g., [1]).

Theorem 1 allows us to solve GPI in P for a class of groups that we now describe. Following [5], we say that a group G has a *Sylow tower* if there is a normal series $\mathrm{id} = G_\ell \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ where each G_i/G_{i+1} is isomorphic to a Sylow subgroup of G . We say that G has an *elementary Abelian Sylow tower* if furthermore all its Sylow subgroups are elementary Abelian.

Corollary 2. *The coset of isomorphisms between two groups G, H can be computed in polynomial time when (1) $\mathrm{Rad}(G)$ has an elementary Abelian Sylow tower, and (2) for any prime p dividing $|\mathrm{Rad}(G)|$, the Sylow p -subgroup of $G/\mathrm{Rad}(G)$ is cyclic, dihedral, semi-dihedral, or generalized quaternion.*

Proof. The algorithm of [3] computes the coset of isomorphisms for groups of the form $G/\mathrm{Rad}(G)$. Apply Theorem 1 iteratively, with this as the base case.

To ensure that the condition is satisfied iteratively, we need the following fact. Let $\mathrm{id} = G_\ell \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ be the filtration where $G_1 = \mathrm{Rad}(G)$ and the rest is an elementary Abelian Sylow tower. Suppose at the i th step, $i \geq 1$, G_i/G_{i+1} is an elementary Abelian p_i -group. We need to show that the Sylow p_i -subgroup G/G_i is isomorphic to the Sylow p_i -subgroup of G/G_1 .

The preceding fact follows from the claim: If N is a normal subgroup of G , and $p \nmid |N|$, then a Sylow p -subgroup of G/N is isomorphic to a Sylow p -subgroup of G . The claim follows from the Schur–Zassenhaus Theorem, but there is also a more direct, elementary proof, as follows. Let P be a Sylow p -subgroup of G , and consider the restriction of the quotient map $\varphi: G \twoheadrightarrow G/N$ to P . Since $p \nmid |N|$, $P \cap N = 1$, so P is mapped isomorphically onto its image in G/N . Since $p \nmid |N|$, $|P|$ is the largest power of p dividing $|G/N|$, so the image of P under the quotient map $G \twoheadrightarrow G/N$ is a Sylow p -subgroup of G/N . \square

We now compare our result with the previous one in [5]. Firstly, a critical difference is that in our setting we need to deal with both actions and cohomology classes (see Section 3). In the setting of [5], the Schur–Zassenhaus theorem implies that the cohomology classes are always trivial, so this part does not appear in [5] at all. Secondly, to deal with actions (Problem 3), though we follow the algorithmic framework of [5], for the supporting algorithmic subroutines, we need to use some sophisticated algorithms in computational algebra (see Section 2), while in [5] the corresponding subroutines are rather straightforward. Finally, we bound the running time of our algorithms by proving size bounds on representations and on group cohomology in the tame case, using an explicit description of representations from the literature, and using previously known results on group cohomology. This was not needed in [5].

More broadly, to achieve Theorem 1, for the first time in the worst-case analysis of GPI, we step into the regime of modular representation theory—that is, when the characteristic of the underlying field divides the order of the group. This theory is much less well-understood than ordinary representation theory. As the reader may see later, to solve Problem 1 in general seems to require certain deep use of this theory. We hope this article serves as a first step in this direction.

Organization. We first present some preliminaries in Section 2. In Section 3 we show how the splitting strategy of [24] applies in this case, and in Section 4 we give an overview of the proofs. Detailed proofs for the action aspect and the cohomology aspect are presented in Section 5 and Section 6. Finally, in Section 7 we discuss the general relationship between GPI and the tame-wild dichotomy in representation theory, and present some open questions. The appendix is devoted to reproduce Crawley-Boevey’s description of the indecomposable modules of semi-dihedral algebras for readers’ convenience.

2 Preliminaries

Notations and definitions. For a prime p , \mathbb{F}_p denotes the field of size p . The characteristic of a field \mathbb{F} is denoted $\text{char}(\mathbb{F})$. $M(n, p)$ is the set of $n \times n$ matrices over \mathbb{F}_p , and $\text{GL}(n, p)$ is the group of $n \times n$ invertible matrices of \mathbb{F}_p . For $n \in \mathbb{N}$, $[n] := \{1, \dots, n\}$. $\text{Sym}(\Omega)$ denotes the symmetric group over a set Ω ; when $\Omega = [n]$ we write S_n . A permutation group over Ω is a subgroup of $\text{Sym}(\Omega)$.

\mathbb{Z}_p denotes the cyclic group of order p . A group is elementary Abelian if it is isomorphic to \mathbb{Z}_p^d for some prime p and some integer d . The dihedral groups (of order a power of 2) are $D_{2^m} = \langle x, y \mid x^2 = y^{2^m} = 1, yx = xy^{-1} \rangle$. The semi-dihedral or quasi-dihedral groups are $\text{SD}_{2^m} = \langle x, y \mid x^2 = y^{2^m} = 1, yx = xy^{2^{m-1}-1} \rangle$. The (generalized) quaternion groups are $\text{GQ}_{2^m} = \langle x, y \mid x^2 = y^{2^{m-1}}, yx = xy^{-1} \rangle$. D_{2^m} , SD_{2^m} , and GQ_{2^m} are of order 2^{m+1} ; D_{2^1} is the Klein four group.

Remark 1. There is a polynomial-time algorithm to decide whether a given group is D_{2^m} , SD_{2^m} , or GQ_{2^m} , because these groups are generated by two elements.

General group theory. A p -group for p prime is a group whose order is p^d for some d . A Sylow p -subgroup of a group G is a maximal p -subgroup of G , under inclusion. Two of the Sylow theorems say that every finite group has a Sylow p -subgroup whose order is the largest power of p that divides G , and all Sylow p -subgroups of G are conjugate to one another. Thus, up to isomorphism, we may speak of “the” Sylow p -subgroup of a group G . Given the Cayley table of a group, a Sylow p -subgroup can be found in polynomial time.

A subgroup N of G is *characteristic* if N is sent to itself by every automorphism of G . A *characteristic subgroup functor* is a function \mathcal{S} from finite groups to finite groups such that (1) $\mathcal{S}(G) \leq G$ for all G , and (2) any isomorphism $\varphi: G_1 \rightarrow G_2$ restricts to an isomorphism $\varphi|_{\mathcal{S}(G_1)}: \mathcal{S}(G_1) \rightarrow \mathcal{S}(G_2)$. In particular, it follows that $\mathcal{S}(G)$ is always characteristic in G . Examples of characteristic subgroup functors include most “natural” characteristic subgroups such as the center, the derived subgroup, and the terms of the derived, lower central, and upper central series. A characteristic subgroup functor is Abelian (resp. elementary Abelian), if $\mathcal{S}(G)$ is Abelian (resp., elementary Abelian) for all G .

Convention: In this paper, whenever we say “characteristic subgroup” we mean the image of an implied characteristic subgroup functor.

Indecomposable modules. As representations of a group Q over a field \mathbb{F} are the same as modules over the group algebra $\mathbb{F}Q$, we shall use the terms module and representation interchangeably. For two representations θ and η , we use $\theta \cong \eta$ to denote that they are equivalent. Let M be a module of an algebra L . M is *indecomposable* if it cannot be written as a direct sum of two submodules. We denote the set of d -dimensional indecomposable modules of an algebra L by $\text{Ind}(L, d)$. The decomposition of M into a direct sum of indecomposables is essentially unique:

Theorem 3 (Krull–Schmidt (see, e. g., [8, Theorem 1.4.6])). *Let ϕ and ψ be two linear representations of a group Q . Suppose $\phi = \iota_1^{d_1} \oplus \dots \oplus \iota_\ell^{d_\ell}$ and $\psi = \iota_1^{e_1} \oplus \dots \oplus \iota_\ell^{e_\ell}$, where ι_i ’s are indecomposable and pairwise non-isomorphic, and all $d_i, e_i \geq 0$. Then $\phi \cong \psi$ if and only if $d_i = e_i$ for every $i \in [\ell]$.*

2-cohomology classes. Let Q be a group, and A an Abelian group. An action θ of Q on A is a group homomorphism $Q \rightarrow \text{Aut}(A)$. A 2-cocycle with respect to the action θ is a function $f : Q \times Q \rightarrow A$ satisfying the 2-cocycle identity $f(p, q) + f(pq, r) = \theta_p(f(q, r)) + f(p, qr)$. The set of all 2-cocycles is an Abelian group under pointwise addition, denoted $Z^2(Q, A, \theta)$. Given a function $u : Q \rightarrow A$, the function $b_u(q, q') = u(q) + \theta_q(u(q')) - u(qq')$ is a 2-coboundary $b_u : Q \times Q \rightarrow A$. The set of 2-coboundaries is a subgroup of $Z^2(Q, A, \theta)$, denoted $B^2(Q, A, \theta)$. The quotient group $H^2(Q, A, \theta) := Z^2(Q, A, \theta)/B^2(Q, A, \theta)$ is the group of 2-cohomology classes. For f and g in $Z^2(Q, A, \theta)$, if $f - g \in B^2(Q, A, \theta)$ (representing the same cohomology class), they are called cohomologous, denoted $f \simeq g$.

Preliminaries for algorithms. As customary in permutation group algorithms [44], a permutation group is represented in algorithms by a set of generators. The automorphism group of a group G is represented as a permutation subgroup of $\text{Sym}(G)$. A coset of a permutation group is represented by a single coset representative together with a set of generators for the subgroup. A representation of Q is given by listing the images of $q \in Q$ explicitly. Two representations θ and η are equal, denoted $\theta = \eta$, if $\theta(q) = \eta(q)$ for every $q \in Q$; compare with $\theta \cong \eta$. A 2-cohomology class is represented by a 2-cocycle f , which in turn can be viewed as a matrix over \mathbb{Z}_p of size $d \times |Q|^2$ when $A \cong \mathbb{Z}_p^d$. In the algorithm, we need to test whether two 2-cocycles f_1 and f_2 are cohomologous. This can be done as in [24]; for completeness we present a proof here.

Proposition 4 ([24]). *Given two 2-cocycles f and g with respect to the action $\theta : Q \rightarrow \text{Aut}(A)$ ($A = \mathbb{Z}_p^d$), whether $f \simeq g$ can be decided in time $\text{poly}(|Q|, d, \log p)$.*

Proof. We need to check whether $f - g \in B^2(Q, A, \theta)$. For this, compute a basis of $B^2(Q, A, \theta)$ as a \mathbb{Z}_p -vector space: This can be done by applying the defining equation of 2-coboundaries to a basis of $\{u : Q \rightarrow A\}$, the dimension of which is $d \cdot |Q|$. As we can treat these as vector spaces, we then test whether $f - g$ is in the \mathbb{Z}_p -span of 2-coboundaries (as a vector in a space of dimension $d \cdot |Q|^2$). As a standard algorithmic task in linear algebra, this can be solved efficiently. \square

Theorem 5 (Module isomorphism [14, 10, 31]). *Given two tuples of matrices $(A_1, \dots, A_n), (B_1, \dots, B_n)$, $A_i, B_j \in M(d, p)$, there exists a deterministic $\text{poly}(d, n, \log p)$ -time algorithm that finds $C \in \text{GL}(d, p)$ such that for every $i \in [n]$, $CA_i = B_iC$, if such C exists.*

A matrix algebra is a linear subspace L of $n \times n$ matrices over a field such that L is closed under matrix multiplication ($a, a' \in L \Rightarrow aa' \in L$). The unit group of a ring or algebra A is the set of invertible elements in A , which naturally form a group under multiplication.

Theorem 6 (Finding units in a matrix algebra [11]). *Given a linear basis of a matrix algebra L in $M(d, p)$, a generating set of the unit group of L can be computed deterministically in time $\text{poly}(d, p)$.*

Theorem 7 (Decomposing into indecomposables [14]). *Given a module M over an algebra L over a finite field \mathbb{F} , a direct sum decomposition of M can be computed in time polynomial in the input size and $\text{char}(\mathbb{F})$.*

Theorem 8 (Parametrized setwise transporter problem [5]). *Given a set of generators of $P \leq S_t$, and $S, T \subseteq [t]$ with $|S| = |T| = k$, $P_{S \rightarrow T} := \{\sigma \in P \mid S^\sigma = T\}$ can be computed in time $\text{poly}(t, 2^k)$.*

3 The divide and conquer strategy for Problem 1

Now we briefly recall the divide and conquer strategy from [24], and how it applies to the particular case of Problem 1. Problem 1 requires us to compute isomorphisms of G, H from isomorphisms of $G/\mathbb{Z}_p^d, H/\mathbb{Z}_p^d$. It is then natural to examine how the quotient group G/\mathbb{Z}_p^d and the characteristic subgroup \mathbb{Z}_p^d are related by G ; this is the starting point for the strategy from [24].

Given a group G and an Abelian characteristic subgroup A of G , let $Q := G/A$; we denote this situation $A \hookrightarrow G \twoheadrightarrow Q$ and call G an *extension* of A by Q . The *extension data* of $A \hookrightarrow G \twoheadrightarrow Q$ consists of two functions: the (conjugation) *action* $\theta : Q \times A \rightarrow A$ defined by $(q, a) \rightarrow qaq^{-1}$, and the *2-cocycle* $f_s : Q \times Q \rightarrow A$, depending on a transversal or *section* $s : Q \rightarrow G$ —i.e., an assignment of an element $s(q)$ to each coset $q \in G/A$ —and defined by $f_s(p, q) := s(p)s(q)s(pq)^{-1}$. Note that $\text{Aut}(A) \rtimes \text{Aut}(Q)$ acts naturally on the set of actions (including θ) and the set of 2-cocycles (including f_s).

In Problem 1, we are given two groups G and H , and their respective characteristic subgroups A and B (recall our convention about characteristic subgroup *functors* from Section 2). Note that if $G \cong H$, then $A \cong B$ and $G/A \cong H/B$. We first test whether $A \cong B$; this is easy because they are Abelian. Recall that we are given $\text{Iso}(G/A, H/B)$; if it is empty then $G \not\cong H$. Therefore, at this point we have either determined that $G \not\cong H$, or we have $A \cong B$ (identified as A), and $G/A \cong H/B$ (identified as Q). This is the divide step of the strategy.

But these conditions are not sufficient to conclude $G \cong H$, so we have yet to conquer, as in the following:

Example 1. We give an example of two tame extensions $A \hookrightarrow G \twoheadrightarrow G/A$ and $B \hookrightarrow H \twoheadrightarrow H/B$ with A characteristic in G , B characteristic in H , $A \cong B$, and $G/A \cong H/B$, but $G \not\cong H$. Let $G = D_{4k} = \langle \rho, \tau \mid \rho^{2k} = \tau^2 = 1, \tau\rho\tau = \rho^{-1} \rangle$ be the dihedral group of order $4k$ with k odd, and let $H = \mathbb{Z}_2 \times D_{2k}$. In both groups, the center—a characteristic subgroup—is \mathbb{Z}_2 (which also happens to be the unique maximal normal 2-group); in the case of H this is clear, in the case of G it is the subgroup $\{1, \rho^k\}$. Both groups are thus characteristic extensions of \mathbb{Z}_2 by D_{2k} . Note that the Sylow 2-subgroup of D_{2k} is cyclic of order 2, since k is odd, so these are both tame extensions. Yet $G \not\cong H$; this can be seen by noting that H contains elements h, x with h of order $2k$, x of order 2 such that hx has order k , yet this is not true of G : The only elements in G of order $2k$ are the generators of $\langle \rho \rangle$, and multiplying any of those by an element of order 2 yields another element of order 2.

Since every element of G has a unique expression as $as(q)$ for $a \in A, q \in Q$, $\text{Iso}(G, H)$ embeds as a subgroup of $\text{Aut}(A) \rtimes \text{Aut}(Q)$. When $A \cong \mathbb{Z}_p^d$, we have $\text{Aut}(A) \cong \text{GL}(d, p)$; $\text{Aut}(Q)$ is given to us as part of $\text{Iso}(G/A, H/B)$. By [24, Lemma II.2], $\text{Iso}(G, H)$ consists exactly of those $(\alpha, \beta) \in \text{Aut}(A) \rtimes \text{Aut}(Q)$ that make the two extension data the same.⁹ Following [24], we refer to the problem of computing the coset in $\text{Aut}(A) \times \text{Aut}(Q)$ consisting of elements sending one extension to the other as **EXTENSION DATA PSEUDO-CONGRUENCE** (or **EDPC**):

Problem 2. Let $A \cong \mathbb{Z}_p^d$. Given $\text{Aut}(Q)$ and the extension data (θ, f) and (η, g) of $A \hookrightarrow G \twoheadrightarrow Q$ and $A \hookrightarrow H \twoheadrightarrow Q$, respectively, compute $\{(\alpha, \beta) \in \text{Aut}(A) \times \text{Aut}(Q) : \theta^{(\alpha, \beta)} = \eta, \text{ and } f^{(\alpha, \beta)} \simeq g\}$.

⁹Note here that the condition of characteristic groups is crucial. That is, if A and B are merely normal subgroups, then this does not hold in general. See [24] for details.

On first sight, EDPC asks for (α, β) that sends θ to η and f to g , *simultaneously*. However, note that $f \in H^2(Q, A, \theta)$; that is, to define the space in which f lives relies on θ in the first place. On the other hand, θ has no dependence on f . Therefore, EDPC reduces to solving the following two problems, *in order*:

Problem 3. Suppose we are given a group Q by its Cayley table, $\text{Aut}(Q)$ by a set of generators, and two linear representations $\theta, \eta : Q \rightarrow \text{GL}(d, p)$ by listing images of Q explicitly. Compute a set of generators for the coset $\{(\alpha, \beta) \in \text{GL}(d, p) \times \text{Aut}(Q) \mid \theta^{(\alpha, \beta)} = \eta\}$, in time $\text{poly}(|Q|, p^d)$.

Problem 4. Suppose we are given a group Q by its Cayley table, a representation $\theta : Q \rightarrow \text{GL}(d, p)$ by listing the images of Q explicitly, and two 2-cocycles $f, g : Q \times Q \rightarrow \mathbb{Z}_p^d$ in $Z^2(Q, \mathbb{Z}_p^d, \theta)$. Furthermore we are given a set of generators for $\{(\alpha, \beta) \in \text{GL}(d, p) \times \text{Aut}(Q) \mid \theta^{(\alpha, \beta)} = \theta\}$. Compute a set of generators for the coset $\{(\alpha, \beta) \in \text{GL}(d, p) \times \text{Aut}(Q) \mid f^{(\alpha, \beta)} \simeq g \text{ and } \theta^{(\alpha, \beta)} = \theta\}$, in time $\text{poly}(|Q|, p^d)$.

We shall refer to Problem 3 as ACTION COMPATIBILITY (or ACTCOMP), and Problem 4 as COHOMOLOGY CLASS ISOMORPHISM (or CCISO).

4 Overview of algorithms for ACTCOMP and CCISO

In this section we give an overview of the algorithms for ACTCOMP and CCISO when $\overline{\mathbb{F}}_p Q$ is tame, thereby proving Theorem 1. The complete proof for ACTCOMP is in Section 5 and for CCISO is in Section 6.

The algorithm for ACTCOMP goes as follows: given representations $\theta, \eta : Q \rightarrow \text{GL}(d, p)$, first decompose them into a direct sum of indecomposables (Theorem 7), and group them by isomorphism types (Theorem 5). That is, $\theta = \iota_1^{d_1} \oplus \iota_2^{d_2} \oplus \cdots \oplus \iota_\ell^{d_\ell}$, and $\eta = \iota_1^{e_1} \oplus \iota_2^{e_2} \oplus \cdots \oplus \iota_\ell^{e_\ell}$. (Some d_i 's and/or e_j 's may be 0.) By Theorem 3, $\theta \cong \eta$ if and only if $d_i = e_i$ for all $i \in [\ell]$. To take into account the effect of $\text{Aut}(Q)$, consider the induced action of $\text{Aut}(Q)$ on the indecomposables of $\mathbb{F}_p Q$. Firstly, compute the closure of $I = \{\iota_1, \dots, \iota_\ell\}$ under $\text{Aut}(Q)$ —that is, the set of all indecomposables that are in the $\text{Aut}(Q)$ -orbit of any ι_i —denoted $\text{Clo}(I)$. Viewing $\text{Aut}(Q)$ as a permutation group on the domain $\text{Clo}(I)$, we need to compute the coset in $\text{Aut}(Q)$ that sends those indecomposables in θ of multiplicity m , to those indecomposables in η of multiplicity m , for every $m \in [d]$. For each $m \in [d]$, this is a setwise transporter problem, so applying Theorem 8 sequentially gives an efficient algorithm—provided that we can upper bound the number of indecomposables of dimension d , and thereby $|\text{Clo}(I)|$, by $\text{poly}(|Q|, p^d)$. We prove that for the tame type this holds (Section 5.2), and for wild type it always fails (Section 5.3). This does not follow directly from the definition of the tame–wild dichotomy, since that requires the underlying field to be infinite, whereas we care about representations over a *finite* field and also need an upper bound on the *number* of indecomposables. We are nonetheless able to prove the upper bound we need by using the explicit description of the indecomposable families for tame group algebras due to Crawley-Boevey [16]. This may be viewed as the first main technical contribution of this work. On the other hand, by [41], for the wild type this upper bound fails badly (see Section 5.3). Finally, by Theorem 6 and 5 we can compute, for each $\beta \in \text{Aut}(Q)$ that make θ and η isomorphic, the coset $\alpha \in \text{GL}(d, p)$ that make $\theta^{(\alpha, \beta)} = \eta$.

We then give an algorithm for CCISO that takes the coset of action compatibilities as its input. As for ACTCOMP, the idea is to view the group of action compatibilities as a permutation group on $H^2(Q, \mathbb{Z}_p^d, \theta)$. Then given two 2-cocycles (representing two 2-cohomology classes), the problem

becomes a pointwise transporter problem, a classical problem in permutation group algorithms that is polynomial-time solvable [44]. For this algorithm to be efficient in our setting, we need to upper bound $|H^2(Q, \mathbb{Z}_p^d, \theta)|$ as $\text{poly}(|Q|, p^d)$ when $\overline{\mathbb{F}}_p Q$ is tame. Using some standard cohomological yoga combined with known but deep results on group cohomology [26], we show that, amazingly, this is true. This is the second main technical contribution of this work. This finishes the overview.

5 Algorithm and bounds for ACTION COMPATIBILITY

In this section we give full details for solving the ACTCOMP in the tame case.

5.1 Algorithm for the coset of action compatibilities

To test equivalence of two linear representations over \mathbb{F}_p , by Theorem 3 we just need to compare the multiplicities of the corresponding indecomposables. The difficulty now is how to take into account the effects of $\text{Aut}(Q)$. To tackle this, the key idea is to view $\text{Aut}(Q)$ as a permutation group on a domain consisting of indecomposable representations. Let $\text{Ind}(Q)$ be the set of indecomposable representations of G up to equivalence. For $S \subseteq \text{Ind}(Q)$, we use $\text{Clo}(S)$ to denote the closure of S under $\text{Aut}(Q)$. By applying generators of $\text{Aut}(Q)$ iteratively and checking whether new indecomposables are generated or not using Theorem 5, we have the following breadth-first-search-style algorithm:

Proposition 9. *Given $S \subseteq \text{Ind}(Q)$, $\text{Clo}(S)$ can be computed in time $\text{poly}(|\text{Clo}(S)|)$.*

A trivial upper bound for $|\text{Clo}(S)|$ is $|\text{Ind}(Q)|$, the total number of indecomposables of $\mathbb{F}_p Q$. Another natural bound for $|\text{Clo}(S)|$ utilizes the dimensions of indecomposables in S . Suppose S is finite and $\{d_1, \dots, d_\ell\}$ are the dimensions of indecomposables in S . Then $|\text{Clo}(S)|$ is upper bounded by the sum of the number of indecomposables of dimensions d_1, \dots, d_ℓ , denoted $\text{Ind}(Q, d_1), \dots, \text{Ind}(Q, d_\ell)$.

Theorem 10. *Problem 3 can be solved for representations of Q over \mathbb{F}_p of dimension d when the number of indecomposable $\mathbb{F}_p Q$ -modules of dimension d is bounded by $\text{poly}(|Q|, p^d)$ for all d .*

For the proof, we need one more straightforward observation:

Observation 1.¹⁰ *Let G be a subgroup of $H \rtimes K$, let $\pi_K: G \rightarrow K$ denote the natural projection onto K with kernel H , and let G_H denote the intersection $G \cap (H \rtimes 1)$. If $\mathcal{H} \subseteq H \rtimes 1$ generates G_H and $\mathcal{K} \subseteq K$ generates $\pi_K(G)$, and for each $k \in \mathcal{K}$, h_k is such that $(h_k, k) \in G$, then $\mathcal{H} \cup \{(h_k, k) \in G : k \in \mathcal{K}\}$ generates G .*

Proof. Given $(h, k) \in G$, first we write k as a word in the generators \mathcal{K} , say $k = k_1 \cdots k_\ell$, with each $k_i \in \mathcal{K}$. Then $(h, k) \cdot ((h_{k_1}, k_1)(h_{k_2}, k_2) \cdots (h_{k_\ell}, k_\ell))^{-1}$ is of the form $(h', 1)$, which is in G_H . Write $(h', 1)$ as a word in \mathcal{H} . \square

Proof of Theorem 10. Given two d -dimensional representations θ, η of Q over \mathbb{F}_p , use Theorem 7 and Theorem 5 to decompose and group by isomorphism types as $\phi = \iota_1^{d_1} \oplus \cdots \oplus \iota_\ell^{d_\ell}$, and $\psi = \kappa_1^{e_1} \oplus \cdots \oplus \kappa_{\ell'}^{e_{\ell'}}$. Let $\text{Ind}(\phi) = \{\iota_1, \dots, \iota_\ell\}$, and similarly we have $\text{Ind}(\psi)$.

¹⁰Essentially this observation appeared as [5, Claim 1], but that formulation was only for direct products, not semi-direct products, and there was a typo in its formulation there. This observation is also used in the journal version of [24]. We include the short proof here for completeness.

For any $\beta \in \text{Aut}(Q)$, $\theta^\beta = (\iota_1^\beta)^{d_1} \oplus \cdots \oplus (\iota_\ell^\beta)^{d_\ell}$. If $\theta^\beta \cong \eta$, then by Theorem 3, $\ell = \ell'$ and there exists $\sigma \in S_\ell$ such that $\iota_{\sigma(i)}^\alpha = \kappa_i$ and $d_{\sigma(i)} = e_i$. Furthermore, this also implies that $\text{Clo}(\text{Ind}(\phi)) = \text{Clo}(\text{Ind}(\psi))$.

Given $\theta = \iota_1^{d_1} \oplus \cdots \oplus \iota_\ell^{d_\ell}$, and $\eta = \kappa_1^{e_1} \oplus \cdots \oplus \kappa_{\ell'}^{e_{\ell'}}$, first check whether $\ell = \ell'$ and $\text{Clo}(\text{Ind}(\theta)) = \text{Clo}(\text{Ind}(\eta))$. If either of these two conditions is not satisfied, then θ and η cannot be equivalent under any $\beta \in \text{Aut}(Q)$. If these two conditions are satisfied, let $\Omega = \text{Clo}(\text{Ind}(\theta))$. The action of $\text{Aut}(Q)$ on Ω allows us to consider $\text{Aut}(Q)$ (or, more precisely, its homomorphic image) as a permutation group $A_Q \leq \text{Sym}(\Omega)$. View ϕ and ψ as functions from Ω to \mathbb{N} , that is, $\phi(\iota)$ is the multiplicity of ι in ϕ . Our task now is just to decide whether there exists $\sigma \in A_Q$ such that for each multiplicity m , σ sends those indecomposables in ϕ of multiplicity m to those indecomposables in ψ of multiplicity m . This is clearly a set-wise transporter problem. Solve this iteratively for each multiplicity. This gives a generating set for the coset $\{\beta \in \text{Aut}(Q) \mid \theta^\beta \cong \eta\}$. For each β in the generating set, use Theorem 5 to compute $C \in \text{GL}(d, p)$ such that $C\theta C^{-1} = \eta$, and use Theorem 6 to compute the unit group of η . Collect all the generators, which gives a generating set for $\{\text{GL}(d, p) \times \text{Aut}(Q) \mid \theta^{(\alpha, \beta)} = \eta\}$. This finishes the description of the algorithm.

Decomposing the representations takes time polynomial in d and p , by Theorem 7, which is much better than what we need for our purposes. The application of the setwise transporter algorithm (Theorem 8) takes time $\text{poly}(|\Omega|, 2^d) = \text{poly}(|\text{Clo}(\text{Ind}(\phi))|, p^d)$. If the number of indecomposable modules of dimension d' is bounded by $\text{poly}(|Q|, p^{d'})$ for all d' , and $\dim \iota_i = d_i$, then $|\text{Clo}(\text{Ind}(\phi))|$ is bounded by $\text{poly}(|Q|, \sum_i p^{d_i}) \leq \text{poly}(|Q|, p^d)$. Thus this application of the setwise transporter algorithm takes time polynomial in the input size.

This gives us one element of $\text{Aut}(Q)$ that sends θ to η (up to equivalence), as well as generators of the subgroup of $\text{Aut}(Q)$ that sends θ to itself (up to equivalence). To get the actual coset of action compatibilities, we need a subgroup of $\text{Aut}(A) \times \text{Aut}(Q)$, that is, including data about the linear equivalences. By Observation 1, it is enough to find, for each generator α of the subgroup of $\text{Aut}(Q)$, generators of the subgroup $\{\beta \in \text{Aut}(A) : \theta^{(\alpha, \beta)} = \theta\}$ (note, *equality* here, not merely equivalence).

To do this, we first find a linear spanning set of the linear subspace of $M(d, p)$ consisting of those matrices β such that $\beta\theta(q) = \theta(q^\alpha)\beta$, using linear algebra over \mathbb{Z}_p . This linear subspace is in fact closed under matrix multiplication, as one can easily check, and the subgroup of $\text{Aut}(A)$ we seek is just the group of units of this matrix algebra. From the matrix algebra itself, we can find its group of units in polynomial time (Theorem 6). \square

For future reference we highlight the key criterion needed for the preceding algorithm to run efficiently:

Criterion 1. *For a group Q , there are at most $\text{poly}(|Q|, p^d)$ d -dimensional indecomposable $\mathbb{F}_p Q$ -modules.*

5.2 The number of indecomposable modules of group algebras

We will show that Criterion 1 holds in the tame case, and fails quite badly for *all* wild group extensions.

It should be noted that our results do not follow directly from the tame–wild dichotomy, because we need explicit upper bounds over finite fields, whereas the dichotomy is typically stated over algebraically closed fields and does not provide quantitative bounds. Therefore, we are forced to

use the explicit descriptions of tame group algebras to get such quantitative bounds over finite fields.

Bounds for the case of finite representation type are furnished by the following theorem:

Theorem 11 (Higman [28]; see [17, Theorem 64.1]). *For a group Q , the group algebra $\mathbb{F}_p Q$ is of finite representation type if and only if the Sylow p -subgroup of Q is cyclic. If this holds, then the number of indecomposable $\mathbb{F}_p Q$ -modules is $\leq |Q|$.*

For tame representation type, we require a more detailed analysis. To start with, it is well-known that the representation type of $\mathbb{F}_p Q$ depends on Sylow p -subgroups of Q , even with quantitative bounds:

Proposition 12 (See [9, Proposition 3(1)]). *Let P be a Sylow p -subgroup of Q . Then $|\text{Ind}(\mathbb{F}_p Q, d)| \leq [Q : P] \cdot (\sum_{d'=\lceil d/[Q:P] \rceil}^d |\text{Ind}(\mathbb{F}_p P, d')|)$.*

Proof. Any indecomposable d -dimensional $\mathbb{F}_p Q$ -module M is an $\mathbb{F}_p Q$ -direct summand of some N^Q , where N is an indecomposable $\mathbb{F}_p P$ -module of dimension d' , with $\frac{d}{[Q:P]} \leq d' \leq d$. (Recall that N^Q denotes the induced module of N to Q .) If N is of dimension $d' \leq d$, then N^Q contributes at most $[Q : P]$ non-isomorphic indecomposable $\mathbb{F}_p Q$ -modules of dimension d . The claim then follows. \square

In other words, to show that Q satisfies Criterion 1, it suffices to show that its Sylow p -subgroup P satisfies Criterion 1.

Now we need to provide an explicit upper bound for the tame group algebras. We do this for the semi-dihedral groups SD_{2^m} . The dihedral groups D_{2^m} can be deduced similarly because the structure of its indecomposables are very similar to those of SD_{2^m} . (In fact, the forms of indecomposables for D_{2^m} are a subset of the forms for SD_{2^m} . See [8, Chap. 4.11] and compare with Appendix A.) The generalized quaternion groups GQ_{2^m} are handled by the following proposition, as GQ_{2^m} is a subgroup of index 2 of $\text{SD}_{2^{m+1}}$: it is the subgroup generated by x^2 and xy . Note that this constant 2 is important here.

Proposition 13 (See [9, Proposition 3(2)]). *Let H be a subgroup of Q . Then*

$$|\text{Ind}(\mathbb{F}_p H, d)| \leq [Q : H] \cdot \left(\sum_{d'=d}^{d \cdot [Q:H]} |\text{Ind}(\mathbb{F}_p Q, d')| \right).$$

Proof. Any indecomposable M of $\mathbb{F}_p H$ of dimension d is a direct summand of the restriction of some $\mathbb{F}_p Q$ indecomposable N of dimension $\leq [Q : H] \cdot d$. Each such N contributes at most $[Q : H]$ non-isomorphic $\mathbb{F}_p H$ indecomposables of dimension d . The result then follows. \square

Proposition 14. $\mathbb{F}_2 \text{SD}_{2^m}$ satisfies the key criterion.

Proof. We shall follow the description of Crawley-Boevey [16]. For the reader's convenience his result is reproduced in Appendix A. Though we try to be self-contained here, a cautious reader is suggested to at least go over Appendix A briefly and return to this proof, since the proof ultimately builds on counting explicitly the specific forms from Crawley-Boevey's construction.

To start with, since Crawley-Boevey's description works over fields of size > 2 , we shall consider $\mathbb{F}_4 \text{SD}_{2^m}$ instead of $\mathbb{F}_2 \text{SD}_{2^m}$. Indeed, as any representation over \mathbb{F}_2 is one over \mathbb{F}_4 via the field

extension, any upper bound on the number of representations over \mathbb{F}_4 will be an upper bound for the number of representations over \mathbb{F}_2 .

The indecomposables of the group algebras $\mathbb{F}_4\text{SD}_{2^m}$ are most easily described in terms of the indecomposables of the so-called semi-dihedral algebra $\Lambda_\ell = \mathbb{F}_4\langle a, b \mid a^3 = b^2 = 0, a^2 = (ba)^\ell b \rangle$, where $\ell = 2^{m-1} - 1$. This is because all indecomposables except the regular one of $\mathbb{F}_4\text{SD}_{2^m}$ are in one-to-one correspondence with those of Λ_ℓ [9].

Briefly speaking, there are four classes of indecomposable modules of Λ_ℓ , called asymmetric strings, symmetric strings, asymmetric bands, and symmetric bands. Each class is associated with a family of configurations, and an auxiliary algebra of finite type. There is a procedure that takes one configuration and one indecomposable module of the auxiliary algebra and produces an indecomposable Λ_ℓ -module. Crawley-Boevey proved that each indecomposable Λ_ℓ -module can be generated by this procedure, and two indecomposables with different configurations or different auxiliary indecomposables are non-isomorphic. Therefore it is enough to deduce an upper bound on the number of indecomposable Λ_ℓ -modules from Crawley-Boevey's description.

Let us detail the case of symmetric strings. To describe the configurations of the symmetric strings, consider words in the alphabet $\{a_i, b_j \mid i \in \{-(\ell+1), \dots, \ell+1\}, j \in \{-1, +1\}\}$, satisfying the following conditions: (1) the letters alternate between a_i 's and b_j 's; (2) there are no subwords of the form $b_1 a_m b_1$, $a_{m+1} b_1$, $b_1 a_{m+1}$, or $a_i b_1 a_j$ where $i, j > 0$. For a letter c_i ($c = a$ or b), $c_i^{-1} = c_{-i}$. For a word $w = w_1 \dots w_n$, define $w^{-1} = w_n^{-1} \dots w_1^{-1}$. Now impose an equivalence relation by identifying w with w^{-1} . If $w = w^{-1}$ then call w symmetric; otherwise w is asymmetric.

The configurations of symmetric strings are derived from the symmetric words. The auxiliary algebra associated with symmetric strings is $\mathbb{F}_4[e]/(e^2 = e)$, which has only two indecomposables E , both are of dimension 1 with e acting as identity and 0, respectively. Therefore, the auxiliary algebra associated with symmetric strings does not play a major role. In contrast, for bands the associated algebra will contribute a notable factor.

Let us consider the case of e being the identity. Given a symmetric word $w = z a_0 z^{-1}$, the rule to construct a Λ_ℓ -module M is explained in Appendix A. Let $d = \dim(M)$. From there it is seen that M is determined by a quiver (a directed graph) with d vertices. The arrows (edges) are determined by z . To get an upper bound on the number of indecomposables from symmetric strings of dimension d , it is enough to note that the vertices can be arranged in a line, with some special gadgets. To start with, note that the arrows among the rightmost $2\ell + 3$ arrows are fixed due to the e -gadget. Then, depending on whether the leftmost arrow is labeled by a or b , whether the remaining arrows are labeled by a or b is also determined. After this, between two adjacent vertices, there can be at most 4 possibilities: (1) an edge pointing left; (2) an edge pointing right; (3) the starting configuration of a_0 -gadget; (4) the ending configuration of a_0 -gadget. Summarizing the above, there are at most $2 \cdot 4^d$ indecomposables of dimension d coming from symmetric strings with e acting as identity. When e acts as 0 the counting task is similar, except that in the e gadget since the image of e is trivial, those vertices in e do not contribute to a dimension. Therefore, summarizing the two cases we have 4^{d+1} is an upper bound. Of course, due to the aforementioned restrictions on the words, and the fact that we need to respect the a_0 -gadget, an arbitrary configuration may not yield a valid word, so $2 \cdot 4^d$ is a very loose bound, but is nonetheless good enough for our purposes.

Similar considerations yield upper bounds for other types.

For asymmetric strings, the auxiliary algebra only contributes two indecomposable, namely the vector space of dimension 1 with identity map, or with the 0 map. Therefore, taking into account the configurations, a representation of dimension d is then determined by a quiver with d vertices

arranged on a line.¹¹ We first have the freedom to set the left-most edge to be labeled by a or b . After this is fixed, for two adjacent vertices, there are 4 possibilities: (1) an edge pointing left; (2) an edge pointing right; (3) the starting configuration of a_0 -gadget; (4) the ending configuration of a_0 -gadget. Therefore 4^{d+1} is an upper bound.

For asymmetric bands, the continuous part is given by Jordan blocks. Since we work over \mathbb{F}_4 , for a fixed dimension d' there are 3 Jordan blocks with nonzero eigenvalues. To count the number of indecomposables arising from asymmetric bands of dimension d , we shall count for each divisor of d separately. This adds a factor of at most d . Now for a fixed decomposition $d = d'n$, we assume the Jordan blocks are of dimension d' , and the rest is to count the number of asymmetric bands with n vertices. Note that we assume the edge between the first two vertices is labeled with b , so for each edge whether it is labeled by a or b will be fixed. As before there are 4 possibilities between two adjacent vertices. Thus $3 \cdot 4^n$ is an upper bound for the decomposition $d = d'n$. Taking into all such decompositions $3d \cdot 4^d$ is then an upper bound.

For symmetric bands, it can be done similarly as for symmetric strings. The main difference is that the indecomposables are from the four-subspace quiver, therefore could possibly contribute a one-parameter family. This can be accommodated as in the case of asymmetric bands, therefore giving a $d \cdot 4^{d+1}$ upper bound. \square

5.3 A lower bound for wild types

We now explain why *every* wild group algebra does not satisfy Criterion 1:

Observation 2 (J. Rickard [41]). *Let $\mathbb{F}_p G$ be a group algebra of wild type. Then there are $p^{\Omega(d^2)}$ indecomposable $\mathbb{F}_p G$ -modules of dimension d .*

Proof. To start with, consider the indecomposable modules of $\mathbb{F}_p \langle x, y \rangle$ —the *non-commutative* polynomial ring in two non-commuting variables x, y with coefficients in \mathbb{F}_p —of dimension d of the following form: fix A to be the single Jordan block of size d . For any matrix B of size d , $(x, y) \rightarrow (A, B)$ gives an indecomposable module of $\mathbb{F}_p \langle x, y \rangle$ of dimension d . There are thus p^{d^2} of such modules. (A, B) and (A, B') are isomorphic, if and only if there exists $C \in \text{GL}(d, p)$ such that $CA = AC$, and $CB = B'C$. The number of $C \in \text{GL}(d, p)$ such that $CA = AC$ is upper bounded by p^d (one can easily compute the set of matrices that commute with a single Jordan block), so the number of non-isomorphic modules of this form is lower bounded by p^{d^2-d} .

Let $\mathbb{F}_p G$ be a group algebra of wild type. By definition,¹² there exists a map from $\mathbb{F}_p \langle x, y \rangle$ -modules to $\mathbb{F}_p G$ -modules, which preserves indecomposability and non-isomorphisms, and multiplies the dimension by some constant depending only on G . Therefore, asymptotically, the number of indecomposables of $\mathbb{F}_p G$ of dimension d is lower bounded by $p^{c \cdot d^2}$ for some constant c . \square

6 Algorithm and bounds for cohomology class isomorphism

In this section we give the full details of the polynomial-time algorithm for CCISO provided that the coset for ACTCOMP is given (i.e., we solve Problem 4 in the tame case). Before we begin, we note that the proofs here use cohomology in a black-box fashion that can be understood by simple pattern-matching, even if the reader is not so familiar with cohomology.

¹¹Here we mean the quiver *after* expansion. Therefore, the drawings for the a_0 gadget and the e gadget need to be rotated 90 degrees for the vertices to be on a line.

¹²This follows from the precise definition wildness, see [8, Sec. 4.4].

Theorem 15. *Let \mathcal{S} be an Abelian characteristic subgroup functor. Given two groups G_1, G_2 , and the coset of action compatibilities for the actions θ_i of $G_i/\mathcal{S}(G_i)$ on $\mathcal{S}(G_i)$, one can determine the coset of isomorphisms $\text{Iso}(G_1, G_2)$ in time polynomial in $|H^2(G_i/\mathcal{S}(G_i), \mathcal{S}(G_i), \theta_i)|$.*

Proof. Let α be an action compatibility, and let $\alpha_1, \dots, \alpha_k$ generate the group of self-compatibilities for the action associated to G_2 . By applying α to G_1 , we may assume that $\alpha = 1$. Now we treat each α_i as a permutation on $H^2(G/\mathcal{S}(G), \mathcal{S}(G), \theta)$. Compute the 2-cohomology classes of the extensions $\mathcal{S}(G_i) \hookrightarrow G_i \twoheadrightarrow Q_i$, and now check if they are in the same orbit of the permutation group generated by the α_i acting on H^2 . The latter is an instance of the pointwise transporter problem, which can be solved in time polynomial in the domain size [44]. One element taking a 2-cohomology class to the other provides an isomorphism, and the stabilizer of the 2-cohomology class gives generators of the automorphism group. \square

To get Theorem 1 from the preceding one, we will show that the following criterion holds in both finite and tame types. Then Theorem 10 is used to find the coset of action compatibilities, and Theorem 15 is used to find the coset of group isomorphisms.

In the rest of this section, instead of writing $H^2(Q, \mathbb{Z}_p^k, \theta)$, we understand θ as defining a module M over $\mathbb{F}Q$, and write $H^2(Q, M)$.

Criterion 2. *The size of $H^2(Q, M)$ is bounded by $\text{poly}(|Q|, |M|)$. Equivalently, the dimension of $H^2(Q, M)$ over \mathbb{F}_p is bounded by $O(\dim_{\mathbb{F}_p} M + \log_p |Q|)$.*

The rest of this section is devoted to showing that in the finite and tame cases we in fact get the stronger statement that $\dim H^2(Q, M) \leq O(\dim M)$. We start with the case of finite type:

Lemma 1 (See [26, Lemma 3.5]). *Let \mathbb{F} be a field of characteristic p , and let Q be a group with a cyclic Sylow p -subgroup. If M is an indecomposable $\mathbb{F}Q$ -module, then for any $j \geq 0$, we have $\dim_{\mathbb{F}} H^j(Q, M) \leq 1$.*

Proposition 16. *Let \mathbb{F} be a field of characteristic p , and let Q be a group with a cyclic Sylow p -subgroup. If M is any $\mathbb{F}Q$ -module, then for any $j \geq 0$, we have $\dim_{\mathbb{F}} H^j(Q, M) \leq \dim_{\mathbb{F}} M$.*

Proof. Write $M = \bigoplus_{i=1}^k M_i$ where the M_i are indecomposable. Since $H^j(Q, \bigoplus_i M_i) \cong \bigoplus_i H^j(Q, M_i)$ [8, p. 34], we get that $\dim_{\mathbb{F}} H^j(Q, M)$ is at most the number of indecomposable summands of M , which is at most the dimension of M . \square

The rest of this section is devoted to showing:

Proposition 17. *Let \mathbb{F} be a field of characteristic two. If the Sylow 2-subgroup of a group Q is dihedral, semi-dihedral, or generalized quaternion, then for any $\mathbb{F}Q$ -module M we have $\dim_{\mathbb{F}} H^2(Q, M) \leq 3 \dim_{\mathbb{F}} M$.*

The form of this next lemma is from [26, Lemma 3.8], but the result is a direct consequence of the Lyndon–Hochschild–Serre spectral sequence ([36, p. 337] and [29]) and standard facts about low-dimensional cohomology groups ([36, pp. 354–355] and [30, Lemma 2.1]).

Lemma 2. *Let N be a normal subgroup of Q , \mathbb{F} a field, and M an $\mathbb{F}Q$ -module. Then*

$$\dim H^2(Q, M) \leq \dim H^2(Q/N, M^N) + \dim H^1(Q/N, H^1(N, M)) + \dim H^2(N, M)^Q,$$

where M^N denotes the Q/N -submodule of M consisting of the N -fixed points, and $H^2(N, M)^Q$ denotes the Q -fixed points in $H^2(N, M)$ (note that here Q acts on both N and M).

As in the case of ACTCOMP, for cohomology with coefficients in an $\mathbb{F}_p Q$ -module, we can essentially reduce from Q to its Sylow p -subgroup:

Lemma 3. *Let Q be a finite group, \mathbb{F} a field of characteristic p , and M an $\mathbb{F}Q$ -module. If H is a subgroup of Q that contains a Sylow p -subgroup of Q , then there is an $\mathbb{F}H$ -module W such that, for all $j \geq 0$, $H^j(H, W) \geq H^j(Q, M)$ and $\dim W \leq \dim M$.*

This follows from standard cohomological results; the proof we give here is from [26, Lemma 3.5].

Proof. By [8, Corollary 3.6.10], M is projective relative to H , thus a theorem of Higman [8, Proposition 3.6.4] applies to M . The latter says that M is a direct summand of some module induced from an $\mathbb{F}H$ -module W . By Frobenius reciprocity, W appears in the restriction of M to H , so $\dim W \leq \dim M$. Finally, Shapiro's Lemma (see, e.g., [26, Lemma 3.4]) says that $H^j(H, W) \cong H^j(Q, W_H^Q)$, and as M is a direct summand of W_H^Q , $H^j(Q, W_H^Q) \geq H^j(Q, M)$. \square

Finally, we prove Proposition 17, thereby proving Theorem 15 and Theorem 1.

Proof of Proposition 17. By Lemma 3 it suffices to prove the result in the case when Q itself is dihedral, semi-dihedral, or generalized quaternion; write $Q = G_m \in \{D_{2^m}, SD_{2^m}, GQ_{2^m}\}$. All three of the possibilities for G_m are extensions of the form $\mathbb{Z}_{2^m} \hookrightarrow G_m \twoheadrightarrow \mathbb{Z}_2$. By Lemma 2, we thus have

$$\begin{aligned} \dim H^2(G_m, M) &\leq \dim H^2(\mathbb{Z}_2, M^{\mathbb{Z}_{2^m}}) + \dim H^1(\mathbb{Z}_2, H^1(\mathbb{Z}_{2^m}, M)) + \dim H^2(\mathbb{Z}_{2^m}, M)^{G_m} \\ &\leq \dim H^2(\mathbb{Z}_2, M^{\mathbb{Z}_{2^m}}) + \dim H^1(\mathbb{Z}_2, H^1(\mathbb{Z}_{2^m}, M)) + \dim H^2(\mathbb{Z}_{2^m}, M) \\ &\leq \dim M^{\mathbb{Z}_{2^m}} + \dim H^1(\mathbb{Z}_{2^m}, M) + \dim M \\ &\leq \dim M + \dim M + \dim M \end{aligned}$$

Each of the last two lines follows from the preceding line by Proposition 16. \square

Although this already gives us the algorithmic consequence we need, we show how to extend Proposition 17 to a wider class of groups, in a way that may be useful in future work:

Corollary 18. *Let G be a group with a subnormal series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_c = G$ where each quotient G_i/G_{i-1} is either simple or cyclic. Let F be a field and M an FG -module. Then $\dim_F H^2(G, M) \leq (35/8)c(c+1) \dim_F M$.*

In particular, for the class of groups for which there is such a chain with c bounded by $O(1)$, we get that $\dim H^2(G, M) \leq O(\dim M)$.

Note that, in general, we only have the bound $c \leq \log_2 |G|$, which would only yield the bound $\dim H^2(G, M) \leq O(\log^2 |G| \cdot \dim M)$, whereas Criterion 2 requires a bound of the form $O(\dim M + \log |G|)$.

Proof. We apply the same proof inductively, using a few additional facts about the cohomology of simple groups. First, Guralnick and Hoffman [27] showed that for simple G , any field F , and any FG -module M , $\dim H^1(G, M) \leq (1/2) \dim M$. Second, under the same conditions, Guralnick, Kantor, Kassabov, and Lubotzky [26] showed that $\dim H^2(G, M) \leq 17.5 \dim M$. Third, analogous to Lemma 2, if G is a finite group, N is a normal subgroup, F is a field and M is an FG -module, then $\dim H^1(G, M) \leq \dim H^1(G/N, M^N) + \dim H^1(N, M)^G$. Let $T_i(c)$ be an upper bound on $\dim H^i(G, M)/\dim M$ for all G with a chain of length c .

By mimicking the proof of Proposition 17, we get the following recurrence for $T_2(c)$:

$$\begin{aligned} T_2(c) &\leq 17.5 + 17.5T_1(c-1) + T_2(c-1) \\ T_1(c) &\leq 0.5 + T_1(c-1). \end{aligned}$$

Together with the fact that $T_1(1) \leq 0.5$ and $T_2(1) \leq 17.5$, we get that $T_1(c) \leq c/2$. Plugging into the bound for T_2 , we get that $T_2(c) \leq \frac{35}{2}((c-1)/2+1) + T_2(c-1)$, and therefore $T_2(c) \leq \frac{35}{4} \sum_{i=0}^{c+1} i$, and the result follows. \square

Remark 2. Guralnick, Kantor, Kassabov, and Lubotzky [26] also showed that for any finite group G , any field F , and any *faithful* FG -module M —that is, the only element of G that acts trivially on M is the identity—then $\dim H^2(G, M) \leq 18.5 \dim M$. Together with our results, this suggests that, in these cases, ACTCOMP may be the only real obstacle to GPI.

7 Conclusion

7.1 Discussion

Generally speaking (if somewhat glibly), there are two overarching reasons an instance of an isomorphism problem can be easy (not just group isomorphism): 1) there are very few possible isomorphisms to check, or 2) there aren't very many isomorphism classes and/or they have an explicit classification. Although this is a coarse caricature of reality,¹³ we believe it provides a useful viewpoint. The results of [43, 46, 32] use the classification of Abelian groups (2); the results of [4, 3] roughly fall under (1): The number of isomorphisms is only $n^{O(\log \log n)}$, and then they use dynamic programming, an algorithm for code equivalence, and results on finite simple groups to reduce this to polynomial time; the results of [34, 40, 5] fall under (2) in the strong sense that they rely on the fact that the number of irreducible representations of a group G in characteristic p that doesn't divide $|G|$ is *finite*, and all other representations are direct sums of these; and the results of [35] use an essentially *finite* classification of type (2) to reduce to (1) (see [25]). We show that when (2) holds—of which tameness is a general interpretation—isomorphism can be tested in P.

Because of the universal property of wildness—it is as hard as classifying the representations of *any* finite-dimensional algebra—it is widely believed that an explicit classification is impossible for wild problems. However, this does not rule out structural information, nor does it necessarily rule out efficient algorithms to decide when two points are equivalent under a wild equivalence relation (for example, as in [14, 10, 31]). However, the wild problems that arise in GPI are frequently “wilder than wild” [6] (analogous to a problem being NP-hard but not in NP), and these problems seem to pose a core difficulty for GPI.

The reasons (1) and (2)—or rather, their absence—also partially explain the widely held belief that nilpotent groups of class 2—those G for which G modulo its center is Abelian—are the hardest cases of group isomorphism, despite the lack of a formal reduction. Option (1) is ruled out, because even for p -groups of class 2 (nilpotent groups of class 2 and order a power of the prime p) in which every element is of order p , there are roughly $n^{O(\log n)}$ possible isomorphisms to check.¹⁴ Option (2) is also ruled out, because the p -groups of class 2 form a wild classification problem [45], and in

¹³For example, we recognize that this may not apply to certain algorithms for GRAPHI.

¹⁴This is essentially because $\text{Aut}(\mathbb{Z}_p^k) \cong \text{GL}(k, \mathbb{F}_p)$, which is of size $\sim p^{k^2} = n^{\Theta(\log n)}$.

fact, one that is “strictly wilder” than classifying the representations of finite-dimensional algebras [6].

These facts, the upper bounds in this paper, and the lower bound on the number of indecomposables in wild type, suggest that the border between tame and wild may also be the current border between the easy and hard cases of GPI.

7.2 Open questions

Question 5. *Upgrade Corollary 2 to groups whose radicals have Abelian Sylow towers, that is, drop the requirement that the Sylow subgroups are elementary Abelian.*

Although we believe this is possible, we note that if one tries to use the methods of this paper, they must be used “in a single shot:” an Abelian Sylow tower can always be refined, as in Cannon and Holt [13], to a subnormal series whose quotients are elementary Abelian. However, if the Sylow subgroups were not themselves elementary Abelian, such as $\mathbb{Z}_{p^2}^d$, then the resulting subnormal series will contain more than one factor of the same characteristic, in which case proceeding inductively is likely to *appear* to run into wildness. However, we believe that it may be possible to extend the structure of tameness, and the results that we leveraged here, from $\mathbb{F}_p Q$ -modules to $(\mathbb{Z}/p^k\mathbb{Z})Q$ -modules, which would be enough to handle Abelian subgroups of characteristic p and exponent p^k all at once. (We note that we wouldn’t really think of this approach as truly handling a wild situation, so much as realizing that a particular situation that might seem wild is in fact tame.)

Acknowledgment. We thank Gábor Ivanyos for pointing out to us reference [11]. J. A. Grochow is supported by an SFI Omidyar Fellowship during this work. Y. Qiao is supported by Australian Research Council DECRA DE150100720 during this work.

References

- [1] J. L. Alperin, Richard Brauer, and Daniel Gorenstein. Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups. *Trans. Amer. Math. Soc.*, 151:1–261, 1970.
- [2] László Babai. Automorphism groups, isomorphism, reconstruction. In R. L. Graham, M. Grötschel, and L. Lovász, editors, *Handbook of combinatorics (vol. 2)*, pages 1447–1540. MIT Press, Cambridge, MA, USA, 1995.
- [3] László Babai, Paolo Codenotti, Joshua A. Grochow, and Youming Qiao. Code equivalence and group isomorphism. In *Proc. 22nd SODA*, pages 1395–1408, 2011.
- [4] László Babai, Paolo Codenotti, and Youming Qiao. Polynomial-time isomorphism test for groups with no Abelian normal subgroups - (extended abstract). In *ICALP*, pages 51–62, 2012.
- [5] László Babai and Youming Qiao. Polynomial-time isomorphism test for groups with Abelian Sylow towers. In *29th STACS*, pages 453 – 464. Springer LNCS 6651, 2012.
- [6] Genrich R. Belitskiĭ and Vladimir V. Sergeĭčuk. Complexity of matrix problems. *Linear Algebra Appl.*, 361:203–222, 2003. Ninth Conference of the International Linear Algebra Society (Haifa, 2001).

- [7] Helmut Bender. Finite groups with dihedral Sylow 2-subgroups. *J. Algebra*, 70(1):216–228, 1981.
- [8] D.J. Benson. *Representations and Cohomology: Volume 1, Basic Representation Theory of Finite Groups and Associative Algebras*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1998.
- [9] V.M. Bondarenko and Yu.A. Drozd. Representation type of finite groups. *Journal of Soviet Mathematics*, 20(6):2515–2528, 1982.
- [10] Peter A. Brooksbank and Eugene M. Luks. Testing isomorphism of modules. *Journal of Algebra*, 320(11):4020 – 4029, 2008.
- [11] Peter A Brooksbank and Eamonn A. O’Brien. Constructing the group preserving a system of forms. *International Journal of Algebra and Computation*, 18(02):227–241, 2008.
- [12] Thomas Bruestle. Typical examples of tame algebras. In *Representations of finite dimensional algebras and related topics in Lie theory and geometry*, volume 40 of *Fields Inst. Commun.*, pages 27–44. Amer. Math. Soc., Providence, RI, 2004.
- [13] John J. Cannon and Derek F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symb. Comput.*, 35:241–267, March 2003.
- [14] Alexander L. Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *ISSAC*, pages 68–74, 1997.
- [15] Keith Conrad. Generalized quaternions. <http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/gen> 2013.
- [16] W. W. Crawley-Boevey. Functorial filtrations III: Semidihedral algebras. *Journal of the London Mathematical Society*, s2-40(1):31–39, 1989.
- [17] C.W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. AMS Chelsea Publishing Series. Interscience Publishers, 1966.
- [18] Ju.A. Drozd. Tame and wild matrix problems. In Vlastimil Dlab and Peter Gabriel, editors, *Representation Theory II*, volume 832 of *Lecture Notes in Mathematics*, pages 242–258. Springer Berlin Heidelberg, 1980.
- [19] V. Felsch and J. Neubüser. On a programme for the determination of the automorphism group of a finite group. In Pergamon J. Leech, editor, *Computational Problems in Abstract Algebra (Proceedings of a Conference on Computational Problems in Algebra, Oxford, 1967)*, pages 59–60, Oxford, 1970.
- [20] I. M. Gel’fand and V. A. Ponomarev. Problems of linear algebra and classification of quadruples of subspaces in a finite-dimensional vector space. In *Hilbert space operators and operator algebras (Proc. Internat. Conf., Tihany, 1970)*, pages 163–237. Colloq. Math. Soc. János Bolyai, 5. North-Holland, Amsterdam, 1972.
- [21] Daniel Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980.

- [22] Daniel Gorenstein and John H. Walter. The characterization of finite groups with dihedral Sylow 2-subgroups. I–III. *J. Algebra*, 2:85–151, 218–270, 354–393, 1965.
- [23] Joshua A. Grochow. Matrix isomorphism of matrix Lie algebras. In *IEEE Conference on Computational Complexity*, pages 203–213, 2012. Also available as arXiv:1112.2012 and ECCC TR11-168.
- [24] Joshua A. Grochow and Youming Qiao. Algorithms for group isomorphism via group extensions and cohomology. In *IEEE Conference on Computational Complexity (CCC14)*, pages 110–119, 2014. Also available as arXiv:1309.1776 [cs.DS] and ECCC Technical Report TR13-123. Submitted for journal publication.
- [25] Joshua A. Grochow and Youming Qiao. On p -group isomorphism and the tame-wild dichotomy. In preparation, 2015.
- [26] Robert Guralnick, William M. Kantor, Martin Kassabov, and Alexander Lubotzky. Presentations of finite simple groups: profinite and cohomological approaches. *Groups Geom. Dyn.*, 1(4):469–523, 2007. Preprint available as arXiv:0711.2817v1 [math.GR].
- [27] Robert M. Guralnick and Corneliu Hoffman. The first cohomology group and generation of simple groups. In *Groups and geometries (Siena, 1996)*, Trends Math., pages 81–89. Birkhäuser, Basel, 1998.
- [28] D. G. Higman. Indecomposable representations at characteristic p . *Duke Math. J.*, 21(2):377–381, 06 1954.
- [29] D. F. Holt. Exact sequences in cohomology and an application. *J. Pure Appl. Algebra*, 18(2):143–147, 1980.
- [30] D. F. Holt. On the second cohomology group of a finite group. *Proc. London Math. Soc. (3)*, 55(1):22–36, 1987.
- [31] Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM J. Comput.*, 39(8):3736–3751, 2010.
- [32] Telikepalli Kavitha. Linear time algorithms for Abelian group isomorphism and related problems. *J. Comput. Syst. Sci.*, 73(6):986–996, 2007.
- [33] Johannes Köbler, Uwe Schöning, and Jacobo Torán. *The graph isomorphism problem: its structural complexity*. Birkhauser Verlag, Basel, Switzerland, 1993.
- [34] François Le Gall. Efficient isomorphism testing for a class of group extensions. In *Proc. 26th STACS*, pages 625–636, 2009.
- [35] Mark L. Lewis and James B. Wilson. Isomorphism in expanding families of indistinguishable groups. *Groups - Complexity - Cryptology*, 4(1):73110, 2012.
- [36] Saunders MacLane. *Homology*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the 1975 edition.

- [37] Gary L. Miller. On the $n^{\log n}$ isomorphism technique (a preliminary report). In *Proc. 10th ACM STOC*, pages 51–58, New York, NY, USA, 1978. ACM Press.
- [38] Ketan Mulmuley. On P vs. NP and geometric complexity theory. *J. ACM*, 58(2):5, 2011.
- [39] L. A. Nazarova. Representations of a tetrad. *Izv. Akad. Nauk SSSR Ser. Mat.*, 31:1361–1378, 1967.
- [40] Youming Qiao, Jayalal M. N. Sarma, and Bangsheng Tang. On isomorphism testing of groups with normal Hall subgroups. In *Proc. 28th STACS*, pages 567–578, 2011.
- [41] Jeremy Rickard. Answer to: the number of indecomposable modules of finite groups over finite fields of a fixed dimension. <http://mathoverflow.net/a/194773/8012>.
- [42] David Rosenbaum. Bidirectional collision detection and faster algorithms for isomorphism problems. arXiv:1304.3935 [cs.DS], 2013.
- [43] Carla Savage. An $O(n^2)$ algorithm for Abelian group isomorphism. Technical report, North Carolina State University, 1980.
- [44] Ákos Seress. *Permutation Group Algorithms*. Cambridge University Press, 2003.
- [45] V. V. Sergeïčuk. The classification of metabelian p -groups. In *Matrix problems (Russian)*, pages 150–161. Akad. Nauk Ukrain. SSR Inst. Mat., Kiev, 1977.
- [46] Narayan Vikas. An $O(n)$ algorithm for Abelian p -group isomorphism and an $O(n \log n)$ algorithm for abelian group isomorphism. *J. Comput. Syst. Sci.*, 53(1):1–9, 1996.

A Indecomposable modules of semi-dihedral groups

In this appendix, to help make the paper more self-contained, we present the description of indecomposables of the semi-dihedral algebra over \mathbb{F}_4 as given by Crawley-Boevey [16], with the aim of determining an explicit upper bound on the number of indecomposables of a fixed dimension.

Recall that the semi-dihedral algebra is $\Lambda_\ell = \mathbb{F}_4\langle a, b \mid a^3 = b^2 = 0, a^2 = (ba)^\ell b \rangle$, where $\ell = 2^{m-1} - 1$. Let λ, μ be two nonzero field elements in \mathbb{F}_4 . The indecomposable Λ_ℓ -modules are classified into four types: asymmetric strings, symmetric strings, asymmetric bands, and symmetric bands. Each type will be associated with a set of configurations, and an auxiliary algebra.

Auxiliary algebras. We first introduce some algebras and their indecomposables.

1. $A = \mathbb{F}$: modules over \mathbb{F} are just vector spaces over \mathbb{F} , and the only indecomposable is thus the one-dimensional vector space \mathbb{F} .
2. $A = \mathbb{F}[x]/(q(x))$, $q(x)$ a quadratic polynomial with distinct roots: two indecomposable modules corresponding to two possible eigenspaces of x .
3. For asymmetric bands, $A = \mathbb{F}[x, x^{-1}]$: indecomposables are given by Jordan blocks of arbitrary dimension with nonzero eigenvalue.

4. For symmetric bands, $A = \mathbb{F}\langle x, y \rangle / (p(x), q(x))$, where $\mathbb{F}\langle x, y \rangle$ denotes the non-commutative polynomial ring, and $p(x)$ and $q(x)$ are quadratic (univariate) polynomials with distinct roots: the indecomposables come from the four-subspace quiver with an extra conditions, namely the pair of subspaces as eigenspaces of $p(x)$ (resp. $q(x)$) are complementary. For the four-subspace quiver, it is well-known that for each dimension vector there is at most one one-parameter family [39, 20] (see [12, Section 3.2] for more recent coverage).

For asymmetric strings, the auxiliary algebra is \mathbb{F}_4 . For symmetric strings, it is $\mathbb{F}_4[e]/(e^2 = e)$. For asymmetric bands, it is $\mathbb{F}_4[x, x^{-1}]$. For symmetric bands, it is $\mathbb{F}_4\langle e, f \rangle / (e^2 = e, f^2 = f)$.

Configurations. To start with, we consider the words in the alphabet $\{a_i, b_j \mid i \in \{-(\ell + 1), \dots, \ell + 1\}, j \in \{-1, +1\}\}$ that alternate between a_i 's and b_j 's. For a letter c_i ($c = a$ or b), $c_i^{-1} = c_{-i}$. For a word $w = w_1 \dots w_n$, define $w^{-1} = w_n^{-1} \dots w_1^{-1}$. For two words w and v , their product is $w \cdot v = wv$, the concatenation of w and v . The k th power of w can then be defined. Furthermore, a partial ordering of words is introduced as follows: $w < w'$, if (1) $w = w'c_i x$ with $i > 0$ for some word x ; (2) $w' = wc_i x$ with $i < 0$ for some word x ; (3) $w = xc_i y$, $w' = xc_j z$, where $i > j$, and x, y, z are words.

To define strings, we further impose conditions and equivalence relations to the above words. The condition is that there should be no subwords of the form $b_1 a_m b_1$, $a_{m+1} b_1$, $b_1 a_{m+1}$, or $a_i b_1 a_j$ where $i, j > 0$. The equivalence relation identifies w with w^{-1} . If $w = w^{-1}$ then call w a symmetric string; otherwise w is an asymmetric string.

To define bands, we also impose conditions and equivalence relations on the words that are of even length, and not powers. The conditions is that, no powers include subwords of any of the four types as in the condition for strings. The equivalence relation is identifying w with all cyclic rotations of w and w^{-1} .

For each string or band, we first associate a preliminary quiver (a directed graph) with edges labeled as follows. Recall that we use c to denote either a or b .

Asymmetric strings Let $w = w_1 \dots w_n$ be an asymmetric string. The quiver is the graph with $n + 1$ vertices $\{v_1, \dots, v_{n+1}\}$, with n edges between v_i and v_{i+1} for $i \in [n]$. The edge E_i between v_i and v_{i+1} is directed towards v_i if and only if $w_i = c_j$ with $j > 0$, or $j = 0$ and $w_{i-1}^{-1} \dots w_1^{-1} > w_{i+1} \dots w_n$. For $w_i = c_j$, E_i is labeled with $c_{|j|}$.

Symmetric strings Let $w = z a_0 z^{-1}$ be a symmetric string, where $z = z_1 \dots z_n$. The quiver is the graph with $n + 1$ vertices $\{v_1, \dots, v_{n+1}\}$, with $n + 1$ edges, including n edges between v_i and v_{i+1} for $i \in [n]$, and a self-loop at v_{n+1} . The edge E_i between v_i and v_{i+1} is directed towards v_i if and only if $w_i = c_j$ with $j > 0$, or $j = 0$ and $z_{i-1}^{-1} \dots z_1^{-1} > z_{i+1} \dots z_n a_0 z$. For $z_i = c_j$, E_i is labeled with $c_{|j|}$. The self-loop is labeled with e .

Asymmetric bands Let $w = w_1 \dots w_n$ be an asymmetric band. By rotating and possibly inverting we assume $w_1 = b_1$. The quiver is the graph with n vertices $\{v_1, \dots, v_n\}$, with n edges between v_i and v_{i+1} for $i \in [n - 1]$, and between v_n and v_1 . The edge E_i between v_i and v_{i+1} is directed towards v_i if and only if $w_i = c_j$ with $j > 0$, or $j = 0$ and $w_{i-1}^{-1} \dots w_1^{-1} w_n^{-1} \dots w_{i+1}^{-1} > w_{i+1} \dots w_n w_1 \dots w_{i-1}$. For $i = 1$, E_1 is labeled with $b = x$. For $i > 1$, $w_i = c_j$, E_i is labeled with $c_{|j|}$.

Symmetric bands Let $w = za_0z^{-1}$ (after a possible rotation) be a symmetric band for some word $z = z_1 \dots z_n$. The quiver is the graph with $n + 1$ vertices $\{v_1, \dots, v_{n+1}\}$, with $n + 2$ edges, including n edges between v_i and v_{i+1} for $i \in [n]$, and 2 self-loops at v_1 and v_{n+1} , respectively. The edge E_i between v_i and v_{i+1} is directed towards v_i if and only if $z_i = c_j$ with $j > 0$, or $j = 0$ and $w_{i-1}^{-1} \dots w_1^{-1} w_n^{-1} \dots w_{i+1}^{-1} > w_{i+1} \dots w_n w_1 \dots w_{i-1}$. For $z_i = c_j$, E_i is labeled with $c_{|j|}$. The self-loop at v_1 (resp. v_{n+1}) is labeled with f (resp. e).

The preliminary quivers need to be augmented with the following three types of gadgets associated with (1) a_i , $|i| > 1$; (2) a_0 ; (3) e (and f). That is, when an edge between is labeled with a_i (resp., a_0 , e , f), it needs to be replaced by the following gadgets. For future use, let $a = a_1$ and $b = b_1$. In the following diagram, we use V , V_i , and I_j as labels of the vertices, because as seen later, these vertices will be eventually labeled by vector spaces which are modules of the auxiliary algebras.

$$\dots V \xleftarrow{a} V_1 \xleftarrow{b} V_2 \xleftarrow{a} \dots \xleftarrow{b} V_{2i-2} \xleftarrow{a} V \dots$$

Figure 1: The a_i gadget for $|i| > 1$.

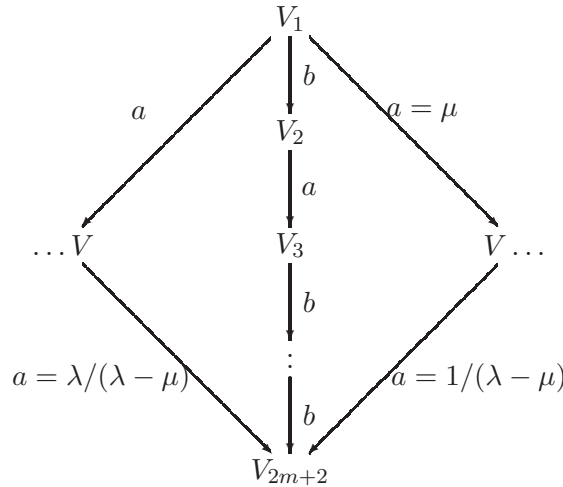


Figure 2: The a_0 gadget.

Now we have all the ingredients to describe the representations of semi-dihedral algebras. For each configuration, we represent it using the preliminary quiver, and expand the preliminary quiver Q' using the gadgets above to get the final quiver Q . Note that after expansion, the possible edge labels in the final quiver Q are: a , b , $b = x$, or $a = y$, where $y \in \{\iota, e, f, \mu, \lambda/(\lambda - \mu), 1/(\lambda - \mu)\}$. Now take an indecomposable V from the corresponding auxiliary algebra. Then a representation of Λ_ℓ can be formed as follows. Let s be the number of vertices in Q . Then the underlying space U is a direct sum of s copies of V . The linear map corresponding to b is specified by interpreting the label b as the identity map between the two copies, and the label $b = x$ as the linear map associated with x , and otherwise 0. The linear map corresponding to a is specified by interpreting

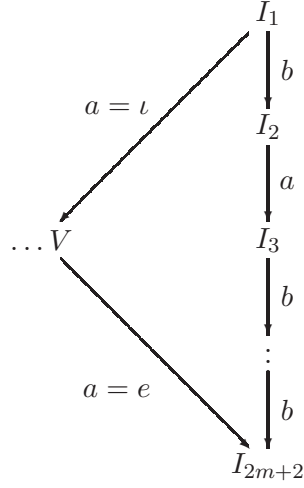


Figure 3: The e (resp. f) gadget. $I_j = \text{Im } e$ (resp. $\text{Im } f$), and ι denotes the inclusion of I_i in V .

label a as identify map, $a = \iota$ as the inclusion map, e (and f) as the idempotent linear map, and $\mu, \lambda/(\lambda - \mu), 1/(\lambda - \mu)$ as the scalar map.

Crawley-Boevey proved that these are all the indecomposables of Λ_ℓ , and if two such indecomposables differ on either the continuous part or the discrete part, they are non-isomorphic.